UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/922,441	02/04/2009	Olivier Courtay	PF050110	6747

24498 7590 02/02/2017

Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
4 Research Way
3rd Floor
Princeton, NJ 08543

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2433	

NOTIFICATION DATE	DELIVERY MODE
02/02/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@technicolor.com
pat.verlangieri@technicolor.com
russell.smith@technicolor.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte OLIVIER COURTAY,
MOHAMED KARROUMI, and ALAIN DURAND

Appeal 2016-003152
Application 11/922,441[1]
Technology Center 2400

Before HUNG H. BUI, JOSEPH P. LENTIVECH, and
SHARON FENICK, Administrative Patent Judges.

FENICK, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants seek our review under 35 U.S.C. § 134(a) of the Examiner's Final Rejection of claims 1–19, all the pending claims in the present application. (Appeal Br. 1.) We have jurisdiction over the appeal under 35 U.S.C. § 6(b)(1).

We AFFIRM.

---

[1] According to Appellants, the real party in interest is THOMSON LICENSING. (Appeal Br. 3.)

Invention

Appellants' invention relates to the secure measurement of round trip time between two devices in a network. (Spec. Abstract.)

Illustrative Claim

Claim 1 is illustrative of Appellants' invention, as reproduced below:

> 1. A method of secure calculation at a first device of time based distance to a second device in a network, comprising:
>
> sending a first message sent to the second device;
>
> receiving from the second device a second message sent in response to the first message;
>
> calculating the time distance based on the time of transmission of the first message and the time of reception of the second message;
>
> receiving a further message comprising authentication data cryptographically linked to one of: at least the first message, at least the second message, and at least the first message and the second message; and
>
> verifying the authentication data.

Examiner's Rejections and References

(1) Claims 1, 3, 5, 8–10, 12–14, 18, and 19 are rejected under 35 U.S.C. § 102(b) as anticipated by Karaoguz (US 2004/0059914 Al; pub. Mar. 25, 2004). (Final Action 11–14.)

(2) Claims 2, 6, 7, 11, and 15 are rejected under 35 U.S.C. § 103(a) as unpatentable over Karaoguz and Overy et al. (US 2003/0220765 Al; pub. Nov. 27, 2003; "Overy"). (Final Action 14–15.)

(3) Claim 4 is rejected under 35 U.S.C. § 103(a) as unpatentable over Karaoguz and Okamoto (US 2005/0050327 Al; pub. Mar. 3, 2005). (Final Action 16.)

(4) Claims 16 and 17 are rejected under 35 U.S.C. § 103(a) as unpatentable over Karaoguz and Moriyama et al. (US 2004/0198430 Al; pub. Oct. 7, 2004; "Moriyama"). (Final Action 16–17.)

Issues

Appellants raise the following issues:

(A) Did the Examiner err in finding that Karaoguz discloses, "a further message comprising authentication data cryptographically linked to one of: at least the first message, at least the second message, and at least the first message and the second message" as recited in claim 1?

(B) Did the Examiner err in finding that Karaoguz discloses verifying authentication data, as recited in claim 1?

(C) Did the Examiner err in finding that Karaoguz discloses the first message comprising a first cryptographic element, a second message comprising a second cryptographic element, and authentication data calculated based on these elements, as recited in claim 3?

(D) Did the Examiner err in finding that Karaoguz discloses "sending a fourth message to the second device to let it know that the method has been initiated," and, "generating the first cryptographic element," as recited in claim 5?

(E) Did the Examiner err in finding that Karaoguz discloses "validating the calculation of the time based distance to the second device upon successful verification of the authentication data," as recited in claim 8?

(F) Did the Examiner err in finding that Karaoguz discloses transmission over a wired connection, as recited in claim 18?

(G) Did the Examiner err in finding that the combination of Karaoguz and Overy teaches or suggests waiting a predetermined time for the generation of a cryptographic element, as recited in claim 6?

(H) Did the Examiner err in finding that the combination of Karaoguz and Moriyama teaches or suggests transmission over a wired connection, as recited in claim 16?

(I) Did the Examiner err in finding that the combination of Karaoguz and Okamoto teaches or suggests the cryptographic elements as random numbers, and authentication data calculated using the random numbers and dependent on a secret, as recited in claim 4?

ANALYSIS

(A) "a further message comprising authentication data"

The Examiner finds that Karaoguz discloses all the elements of claim 1. (Final Action 11.) Karaoguz relates to an authentication device for authenticating a user of a wireless device and determining location information for the user. (Karaoguz, Abstract.)

Karaoguz discloses the transmission of signals from an authentication device to a customer device, in which the timing of the transmission of the signals, along with other factors, is used to determine location information for the customer, relative to the authentication device. (Karaoguz ¶¶ 22–26, Fig. 3.) This location information can be used to verify customer identity. (*Id.* ¶¶ 36–38, Fig. 3.) Karaoguz additionally discloses that when two wireless devices are to be in an ad hoc wireless network, each may be integrated with authentication features and can each operate as an

authentication device (*id.* ¶ 41), and a first user can receive a request to establish communication and, in the process of responding, can determine location information for a second user (*id* ¶ 42). A received request from a second user to a first user to join an ad hoc network may include the second user's encryption or public key, which may then be used to encrypt all messages sent to the second user. (*Id.*) In subsequent steps, a challenge may be sent, cryptographically encoded, challenging the second user to move from the initially determined location to a new location. (*Id.* ¶ 45.) Once the challenge has been completed by the second user, the second user sends an acknowledgement message to the first user, and the first user can determine, using the location determination procedure, whether the challenge has been met. (*Id.* ¶¶ 46–47.)

Appellants argue that Karaoguz does not describe the content of the acknowledgement message sent by the challenged user (second user) and, as such, cannot comprise "a further message comprising authentication data" as disclosed in claim 1. (Citation)

We disagree. Appellants' focus on the acknowledgement message of Karaoguz in relation to the claimed "further message" is not consistent with the Examiner's findings. The Examiner maps certain steps whereby Karaoguz' first user determines the initial location of a second user to the first and second message of the claim. (Final Action 4, 11; Answer 7–9.) When a second ("challenge") determination of location information for the second user is performed using the same process, transmissions from the first user to the second user in this process include a challenge message encrypted using a cryptographic key. (Karaoguz ¶¶ 45–46.) According to the Examiner, this challenge message (and not the acknowledgement from

the second user) discloses the further message, and that this challenge message is encrypted by the cryptographic key and therefore includes authentication data which is verified. (Final Action 4; Answer 8.)

Because the Examiner cites this challenge message, rather than the acknowledgement message sent back by the second user, as the further message, Appellants' arguments regarding the acknowledgement message are inapposite.

Appellants further argue that the challenge message cannot be the further message, because "that message is sent from the authentication device, not received by it." (Appeal Br. 16.) However, we note that the claim does not require that the further message be sent from or received by a specific one of the claimed first and second devices. As such, we are unpersuaded of error in the Examiner's findings that the Karaoguz challenge message discloses the "further message" of claim 1.

(B) "verifying the authentication data"

Still with respect to claim 1, Appellants further argue that the "verification of the authentication data" disclosed in Karaoguz is Karaoguz' calculation of a second location. (Appeal Br. 16.) Appellants argue that Karaoguz' "sending, receiving, and calculating a second time" cannot disclose the claimed verification of the authentication data sent in a further message, since "the reflected messages in Karaoguz do not comprise any authentication data." (*Id.*)

However, as detailed *supra*, the challenge message is mapped to the "further message" and this message includes cryptographic information which is verified (authenticated) by the second user. Therefore, we are

unpersuaded of error in the Examiner's findings with respect to this claim element.

Thus, we are not persuaded the Examiner erred in rejecting claim 1, and claims 9, 10, and 14, argued on the same basis (Appeal Br. 18, 19). Appellants' arguments with respect to claims 2, 7, 11, 12, and 15 are based on the same deficiencies in the Examiner's obviousness rejection based on Karaoguz in combination with other art (Appeal Br. 21–22), and we are likewise not persuaded of error with respect to those claims.

(C) Claim 3

Claim 3 depends from claim 1, and further recites: "wherein the first message comprises a first cryptographic element and the second message comprises a second cryptographic element, and the authentication data is calculated based on the first and the second cryptographic elements."

Appellants argue that the challenge request of Karaoguz "is not a cryptographic element" and that the acknowledgement returned by the second user after moving location "is not a cryptographic message." (Appeal Br. 17.) At the outset, we note that the messages are claimed to "comprise" cryptographic elements, and thus the Appellants' argument that the challenge request "is not a cryptographic element" is unavailing. We also agree with the Examiner that Karaoguz discloses a first message in which the second user sends a cryptographic key (thus disclosing a message comprising a cryptographic element), and that second (and subsequent) messages sent from the first user to the second user are encrypted with the cryptographic key. (Answer 9.) Appellants assert that "[a]s already admitted by the Examiner, Karaoguz fails to teach the authentication data" and "those skilled in the art understand that authentication data cannot be

based on" the cryptographic elements cited by the Examiner. (Appeal Br. 17.) However, we do not see such an admission by the Examiner and agree with the Examiner that Karaoguz discloses validation which is based, at least in part, on cryptographic keys and data which are used to verify certain messages.

Thus, we are not persuaded that the Examiner erred in rejecting claim 3. Additionally, Appellants' arguments with respect to claim 13 are based in part on similar grounds (Appeal Br. 18–19), and we agree with and adopt the Examiner's findings (Final Action 8–9, 13; Answer 11) and are not persuaded of Examiner error with respect to that claim.

(D) Claim 5

Claim 5 depends from claim 3, and further comprises, "sending a fourth message to the second device to let it know that the method has been initiated; and generating the first cryptographic element."

The Examiner finds that the fourth message is taught or suggested by additional messages, citing Karaoguz at paragraph 38. (Final Action 12.) That paragraph of Karaoguz describes how, for a customer with a location which is determined and verified, the authentication device can send the verified customer cryptography protocols which can be used to establish a wireless communication session. (Karaoguz ¶ 38.)

Appellants argue that the claimed feature "happens at the beginning of the sequence" "implicitly." (Appeal Br. 17; Reply 10). The Examiner, however, finds that according to the broadest reasonable interpretation of the claim in light of the specification, "let[ting the second device] know that the method has been initiated" need not be the first transmission to the second device, but may be disclosed by Karaoguz' message initiating a challenge.

(Answer 10.) We agree with the Examiner that the broadest reasonable interpretation of the claim limitation does not require that the claimed fourth message regarding transmitted knowledge of method initiation occur before any other message, and we are not persuaded of error in the Examiner's rejection of claim 5.

(E) Claim 8

Claim 8 depends from claim 1, and further comprises: "validating the calculation of the time based distance to the second device upon successful verification of the authentication data."

Appellants rely on their arguments regarding verification, addressed *supra*, and additionally note that Karaoguz' distance calculation is performed with two messages and that the challenge initiation is not analyzed by the validating device. (Appeal Br. 18.)

However, we agree with the Examiner that cryptographic verification is used to validate messages exchanged between the first and second user in Karaoguz which are used in the process of calculating location. (Appeal Br. 12.) We agree with and adopt the Examiner's findings with respect to this claim, that the time-based distance is validated cryptographically as described in Karaoguz. (*Id.*) We are not persuaded of error in the Examiner's rejection of claim 8.

(F) Claim 18

Claim 18 depends from claim 10, and further requires "the input/output interface is adapted to be connected to a wired connection."

We initially note that there is no exact antecedent basis for "the input/output interface" of the claim. The Examiner finds this to be taught in Karaoguz' disclosure of a wireless network connected with a LAN by wires

or cables. (Final Action 14.) Appellants argue that "it is clearly not this interface that is used when communicating with the wireless devices." (Appeal Br. 19.) However, claim 18 requires only that an interface in the claimed device is "adapted to be connected to a wired connection," not what is communicated over the connection, if anything, or with which devices such communication might occur. We are therefore not persuaded of error in the Examiner's rejection of claim 18, or of claim 19, argued on the same basis.

(G) Claim 6

Claim 6 depends from claim 5, and further comprises "waiting a predetermined time so as to give the second device time to finish the generation of the second cryptographic element."

The Examiner finds paragraph 27 of Karaoguz teaches the limitation of claim 6. (Final Action 15.) In the Answer, the Examiner additionally finds this limitation to be taught or suggested by Karaoguz's teachings that processing time may be considered in distance calculations. (Answer 12.) Karaoguz teaches that the delay between sending a request and receipt of a response may be calculated considering both transit time and processing time ΔP. (Karaoguz ¶¶ 28–31.) The Examiner's finding regarding waiting for the processing time used to generate a response stands unrebutted by Appellants. (Reply 12.) We are unpersuaded of error in the Examiner's rejection of claim 6.

(H) Claim 16

Claim 16 depends from claim 1, and further recites: "wherein at least one of the first message and the second message is transmitted over a wired connection."

The Examiner finds that Moriyama, in combination with Karaoguz, teaches or suggests this claim limitation. (Final Action 16–17.) Moriyama teaches a wireless connection, which is entered into after authentication over a wired connection path occurs. (Moriyama, Abstract.)

Appellants argue that Moriyama's wired connection would "defeat the entire purpose" of requesting the user to change locations as an authentication challenge, as described in the referenced embodiment of Karaoguz. (Appeal Br. 23.) However, the Examiner finds that the first message, in which a public key may be exchanged, according to Karaoguz, could be exchanged in advance over a wired connection, which would teach or suggest the claim limitation at issue. (Answer 12–13.) Additionally, the Examiner points to the presence in the Karaoguz disclosure of a wired network path, through which certain communications with devices may, in part, be transmitted. (Final Action 10.) We are not persuaded that a transfer of a public key over a wireless connection or messages exchanged in part over wired connections would defeat the location-change challenge, and thus are not persuaded of Examiner error.

Appellants present additional arguments for the first time in the Reply Brief, including that "[t]he Examiner's interpretation means that one of these devices is the access point and the other device . . . is the server on the LAN." These arguments, while couched as responsive to the Examiner's Answer, address findings and remarks which are not substantially different from findings appearing previously in the Final Action. (Final Action 10, 16–17.) Therefore, as these arguments are made for the first time in the Reply, with no showing of good cause, and we do not consider them. 37 C.F.R. § 41.41(b)(2) (2013); *See Ex parte Borden*, 93 USPQ2d 1473, 1474

(BPAI 2010) (Informative) ("[T]he reply brief [is not] an opportunity to make arguments that could have been made in the principal brief on appeal to rebut the Examiner's rejections, but were not.").

Thus we are not persuaded of Examiner error in the rejection of Claim 16, or of claim 17, argued on substantially the same basis.

(I) Claim 4

Claim 4 depends from claim 3, and further recites: "wherein the cryptographic elements are random numbers and the authentication data is a result of a function calculated using the random numbers, the function being dependent on a secret."

The Examiner finds that Okamoto teaches authentication using random numbers. (Appeal Br. 16.) Based on the teachings of Okamoto, the Examiner concludes "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention . . . to include a means to utilize random numbers for authentication." (*Id.*) While Appellants argue that Okamoto teaches the use of only one random number, it is the combination of the teachings of Okamoto as to the use of random numbers in a verification process with the teachings of Karaoguz which teaches or suggests the disputed limitation. The test for obviousness is whether the combination of references, taken as a whole, would have suggested the patentee's invention to a person having ordinary skill in the art. *In re Keller*, 642 F.2d 413, 425 (CCPA 1981). We agree with the Examiner that Okamoto's disclosure regarding the use of random numbers in verification would have taught or suggested the use of such numbers in the Karaoguz system and thus we are not persuaded of error in the rejection of claim 4.

Conclusion

Based on the record before us, we are not persuaded of Examiner error. Therefore, we sustain the Examiner's 35 U.S.C. § 102(b) rejection of claims 1, 3, 5, 8–10, 12–14, 18, and 19, and the 35 U.S.C. § 103(a) rejection of claims 2, 4, 6, 7, 11, 15, 16, and 17.

DECISION

We affirm the Examiner's decision rejecting claims 1, 3, 5, 8–10, 12–14, 18, and 19 under 35 U.S.C. § 102(b).

We affirm the Examiner's decision rejecting claims 2, 4, 6, 7, 11, 15, 16, and 17 under 35 U.S.C. § 103(a).

Pursuant to 37 C.F.R. § 1.136(a)(1)(iv), no time period for taking any subsequent action in connection with this appeal may be extended.

AFFIRMED